DOCUMENT RESUME

ED 417 754 IR 056 990

TITLE	Censorship and the Internet in Schools: Problems and Solutions.
PUB DATE	1996-00-00
NOTE	23p.; Topic A in: Proceedings of the ITEC Virtual Conference: A Meeting of the Minds (Australia, 1996); see IR 056 989.
PUB TYPE	Reports - Descriptive (141) -- Speeches/Meeting Papers (150)
EDRS PRICE	EDRS Price MF01 Plus Postage. PC Not Available from EDRS.
DESCRIPTORS	Access to Information; *Censorship; Computer Mediated Communication; Computer Uses in Education; Educational Planning; *Educational Technology; Electronic Libraries; Elementary Secondary Education; Foreign Countries; *Information Management; *Information Policy; *Information Technology; *Internet

ABSTRACT

Five papers focusing on censorship include: "Censorship: Planning a Safe Ride on the Superhighway" (Daniel Ingvarson); "Censorship and the Need to Develop Policy" (Phil Davidson); "Are You Feeling the Internet Backlash?, or Family Friendly Digital Libraries and Banned URLs Week" (Steve Cisler); "Developing a School Internet Management Plan" (Jack Gilding); and "Management of Student Access to the Internet: Issues and Responsibilities" (Ken Dillon).-(AEF)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 417 754

TOPIC A

CENSORSHIP AND THE INTERNET IN SCHOOLS:

PROBLEMS AND SOLUTIONS

Lyn Hay
James Henri

2A

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☐ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

BEST COPY AVAILABLE

IR056990

CENSORSHIP: PLANNING A SAFE RIDE ON THE SUPERHIGHWAY

Daniel Ingvarson
Director, schools*NET*

What's happening? The dream of a global village with free communication and understanding is being overrun with pornography. Are our students at risk? Is the Internet the perfect place for perverts and paedophiles?

Censorship, it's a nasty word. Few like the idea of restricting information or being the moral judge of a generation. It's tricky ground. What's right for whom and when? We live in a multicultural society with widely diverse opinions and viewpoints. When does education and enlightenment stop and inappropriate access to potentially harmful information start? When does culture override information? When does explanation or instruction become invitation to try dangerous experimentation?

When you consider the media hype and focus on the 'porn' highway and the claims of massive hard core and child pornography, is this superhighway about to roll over our children?

WHAT IS OUT THERE?

Hands up all those who have looked for pornography on the Internet (many people have because of all the media attention on it). I thought I would find out. We have a composite of 27 years of Internet experience in our building and some of the best netsurfers around. So armed with keywords like nude, erotic, sex, bombs, and many more we set out on a 36 hour hunt for the dark side of the Internet. We searched over 11 million pages of the World Wide Web, gopher and FTP. We found 3136 sites which matched our keywords. These were made up of a vast array of sites, including: magazines, self-help pages, community information, and academic discussions. There were 45 indexes to other pornographic sites. These indexes proved to be very frustrating. On some of the lists more than 60% of the sites listed were either no longer available, required you to pay for the images, or just never responded. Of the others many were slow, and the pictures of poor quality and mainly of the nude titillation variety.

There was almost a sigh of relief when the first pictures of people having intercourse were uncovered -- one site with more than 12 hard core pictures. It was a number of hours till we found any more.

Out of the entire search only eight sites were found which had pictures which would be considered as hard core pornography -- four of these sites had fewer than five pictures.

There were a considerable number of sex shops and phone sex sites (which advertises traditional phone sex) -- these would describe products and occasionally have crude selling lines. Most, however, had few erotic images at the site. Some would provide you with titillation of one image and you would have to put in your credit card number to get any more pictures.

In total the number of sites which had considerable pornographic material freely available and easily accessible was less than 100. Out of 11,000,000, that's a percentage of 0.001.

SCHOOLS RESPONSIBILITIES

No one would suggest that a school would condone the distribution of pornographic material, nor would schools assist access to it. This leaves schools in the awkward position of allowing students access to the Internet where pornography is available, and have to control its access. On the one hand censorship is against the ethos of many schools and the Internet community in general, on the other, schools have a duty of care to students. If a school were openly allowing students to gain access to inappropriate material (whatever that may be) many parents and others in the school

BEST COPY AVAILABLE

community would be concerned and upset, often blaming the access to the material directly on the teachers. Perhaps there is the possibility of parents pulling their students from the school. Whatever the case, it is clear that the potential for misunderstanding and blame could be easily blown out of proportion with this sensitive issue. There are four parties involved in dealing with censorship of the Internet. The school, its teachers, the students and their parents. A process must be developed which includes all these parties.

THE PROCESSES

The central responsibility lies with the school. Schools must decide before allowing unsupervised access to students, how they are going to keep all these parties informed of the potential issues and rules which have been established. There are different approaches. However, they all revolve around informing everyone involved of their responsibilities.

There is a need to inform parents and get their consent for their children to gain access. There is a need to build an acceptable use policy and to provide students with an 'Internet drivers licence'. These three documents have been developed and used in a number of schools around Australia and across the world.

ACCEPTABLE USE POLICIES

The Acceptable Use Policy (AUP) is the core of any approach to controlling access. It must encompass what is allowed, what is not, what is done and how. The basic tenets of an AUP are: use the Internet for school work only; follow etiquette and the parental consent form explains to parents how students will be using the Internet; the nature of some of the information available; and the process which students will be asked to follow. Some schools have the parental consent form which is signed by the parent and also counter signed by the student, this is then copied off the form and laminated to make a little card like a library card which becomes the student's Internet driver's licence.

It is important for schools to establish the rules associated with use of the Internet through a formal agreement with the students and their parents.

In looking at the various models in use around the world, certain common elements emerge. We have pulled together a list of the main features to be covered, and include some examples such as an introductory letter to parents from a Victorian high school, a policy taken from a US community high school, and one from a group project in Pittsburgh involving 75 schools.

Main Features of an Acceptable Use Policy (AUP)

1. An introductory letter to parents which explains the Internet, its expanding role, the free access to information, and then the need for an agreement on how it is expected to be used.

2. The policy should cover:
   - who is involved in the agreement;
   - what is considered to be inappropriate use of the Internet;
   - acceptance of personal responsibility for own behaviour on the Internet, and for reporting any misuse discovered in the course of use of the Net;
   - acceptance of access to the Net as a privilege not a right, with inappropriate use resulting in cancellation of the privilege;
   - an outline of the Net etiquette expected;
   - rules to follow for privacy, and security;
   - guidelines of what is acceptable to be published on the Internet; and
   - what to expect if the agreement is breached, of loss of access temporarily or permanently, or requirement of parents to purchase printer cartridges, etc.

There may be two agreements, one for the parents and one for students, couched in relevant language. Or, it may work to combine these with parents and students signing the one agreement.

An Example

The following is the Student Ethics Policy for the Common Knowledge: Pittsburgh project. It was developed by a group of teachers, administrators and students.

Subject: Student Ethics Policy

LETTER TO PARENT(S) OR GUARDIAN(S)

Dear Parent(s) or Guardian(s):

Your son or daughter will get access to a world-wide network called the Internet. The reason for using the Internet is to participate in a curriculum project developed by some of your child's teachers. Your son or daughter will reach this world-wide network through a computer account provided by the Common Knowledge: Pittsburgh (CK:P) project.

Common Knowledge: Pittsburgh is a research project funded by the National Science Foundation. The Pittsburgh Public Schools, the Pittsburgh Supercomputing Center, and the University of Pittsburgh are working together on CK:P.

The purpose of this letter is to give you information about the Student Ethics Policy that Common Knowledge: Pittsburgh will use. The policy is described on page 2.

We ask you to review this policy with your child and to sign the consent form. Your child's teacher has already discussed this policy with your son or daughter.

If you have any questions about the network curriculum activities, please call your child's teacher. If you would like more information about the Common Knowledge: Pittsburgh project, please call the CK:P Education office at 622-5930.

STUDENT ETHICS POLICY, GUIDELINES and PROHIBITIONS

PART ONE The Internet is a world-wide telecommunications network. There are hundreds of resources on the Internet. You will find libraries, government agencies, universities, discussion groups, software, technical information, as well as the 20 million people who are part of this world-wide network. Your student account lets you use these resources.

The purpose of your student account is to let you take part in the curriculum activities, at your school, supported by Common Knowledge: Pittsburgh.

PART TWO The Academic Integrity Policy is part of the Rules of Student Conduct. Item #12 of the Policy talks about Academic Dishonesty. While working on the Internet, you are expected to follow the Rules of Student Conduct and to not violate the Academic Dishonesty clause.

PART THREE Common Knowledge: Pittsburgh will monitor your use of network resources. Monitoring will include tracking the amount of time you spend using these resources, but will not require identifying you by name. Other evaluation activities - classroom observation and interviews - are covered in a separate consent form. (See University of Pittsburgh, Consent to Participate in a Study, attached)

PART FOUR You are expected to exercise responsible behaviour when on the network.

PART FIVE 1. Using someone else's network account is not acceptable. 2. Using your network account for non-school related activities is not acceptable. 3. Using

BEST COPY AVAILABLE

unauthorised copies of commercial software is not acceptable. 4. Copying software provided by Common Knowledge: Pittsburgh is not acceptable (see District's Copyright Policy, attached).

PART SIX Violating the above guidelines and prohibitions will result in losing your network account.

STUDENT ETHICS POLICY CONSENT FORM

I have read the Student Ethics Policy and understand its contents. Any questions I have about the network curriculum activity will be answered by my teacher. Any questions I have concerning the Common Knowledge: Pittsburgh project will be answered by the CK:P Educational Staff (622-5930).

My signature below, and that of my parent(s) or guardian(s), means that I agree to follow the guidelines and prohibitions of the Student Ethics Policy as stated on page 2 - Student Ethics Policy Guidelines and Prohibitions.

Student's Signature: _____

Name of Student: _____

School: _____

Grade: _____

Parent(s) or Guardian(s) Signature: _____

Name of Parent(s) or Guardian(s): _____

Date: _____

WWW Publishing Guidelines

Along with the school policy on who maintains school Web pages, a policy of not identifying or publishing information and pictures of students must be established. A story which brings home the significance of WWW publishing guidelines is when a 15 year old girl was approached by a 16 year old boy on the Internet and asked where she lived. The student refused to give out that information, but agreed to meet the boy in the park. She went along with a few friends and the 16 year old boy turned out to be a 50 year old man. This man had got his information on the girl from the school's WWW site. It had a picture of the girl and her email address. It is important to remember that the Internet is a two way street, your students can get access to information, however, the world can have access to your students, and if you are responsible for them it would be wise to ensure that they understand the real dangers of giving out personal information on the Internet.

Where can I get other examples of AUP's?

The K-12 archive at Rice University in the US has a large group of these policies. Try the URL **<gopher://riceinfo.rice.edu:1170/11/More/Acceptable>**. Or search for AUP.

CONTROLLING ACCESS

Blocking and filtering

Appearing in the market place are software tools which assist schools in controlling access to the Internet. These fall into three basic categories, keyword blocking, site filtering, site allowing. No access control software is perfect so they do not negate the need for an AUP, however, they can help by making access to certain sites much more difficult.

Net Nanny is an example of keyword blocking software. What it does is look for words like sex or bomb and if it finds an appropriate match it blocks access to that information. The strengths are ease of set-up and not having to know which sites contain the information beforehand. Its weakness is that keyword searching is rudimentary. If you are looking at an article on the issues facing the police in dealing with drugs or prosecution it could be blocked because of the keywords in the document. You can find out more about *Net Nanny* at **<http://www.netnanny.com>**.

Surfwatch is an example of site blocking software. It has a list of sites which are known to contain inappropriate material. If a student attempts to access that site the software will stop them. Its strengths are the list of inappropriate sites as updated by *Surfwatch*. The down side is that you have to pay for updates and you have little control over what gets blocked. More information on *Surfwatch* can be found at **<http://www.surfwatch.com Site>**.

CensorNet is a site allowing software. It blocks every site on the Internet unless you say that site is OK to access. This is the most restrictive type of blocking and there would be less chance of students gaining access to inappropriate sites this way, however, this also means that most new sites would also be blocked until individually sanctioned as OK by the teachers. More information can be found at **<http://www.ats.com.au/CensorNet>**.

All the above software is designed for the home market and is loaded onto each computer. Another approach is to have a server which connects all the computers in a school (see section on Connecting your school to the Internet) and which does the site blocking. One such product is *CensorMan*, this allows for simple maintenance of the access control from one point. For more information on *CensorMan* try **<http://www.schnet.edu.au /schnet/software.html>**.

GUIDELINES FOR SAFE INTERACTION

Probably the most useful thing that an adult can do for children concerning the Internet is teach them how to safely interact online. It is no different than teaching a child about looking both ways before crossing the street and not talking to strangers. Below are my guidelines for safe enjoyment.

- ***For children under a certain age (14 for instance) a parent must always be in the room while the computer is on.***

This is a good idea even for the simple reason of physical safety. These children are dealing with electrical equipment and could potentially hurt themselves or the computer through ordinary curiosity. For online interaction think of it as a responsibility equivalent to telling a child to always hold an adult's hand when crossing the street.

- ***Take the time to talk with your children about what they are experiencing online.***

When I was growing up both of my parents worked. Nevertheless, they always found time to speak with us about what we had been reading or watching on TV. This is invaluable for teaching children analytical thinking which will help them with their school work. It will also give you an idea of what they are getting into. It is important to keep these conversations uncritical and supportive, genuinely listen and be interested in their explorations. When you find they have come across material you disapprove of, make it an opportunity to explain your values rather than shaming your children for seeing something wrong. How better to safely prepare them for the world beyond school?

- ***Impress upon your children that they must not give out personal information such as their telephone number or address online.***

BEST COPY AVAILABLE

When making friends with people on the Internet the temptation to give out such details about yourself can be great. After all when you or your children feel they are benefiting from a relationship, it is only natural to want to extend that relationship. It is possible to do this safely, but giving out details online is not one of them.

- ***When meeting with online friends for the first time, children must always have an adult present.***

People who meet on BBSs (Bulletin Board Systems, the hobbyist equivalent of the Internet), mailing lists or UseNet newsgroups often organise get-togethers such as barbecues to meet one another. Upon occasion I will even meet with someone individually that I have enjoyed chatting with by email, but only with the added company of a trusted male friend. You may feel you know somebody by their words, but until you meet with them in person you can't know for sure how honest they have been. Group situations are preferable, such as a picnic, barbecue or party, though for young people such a first time gathering should still have the presence of a trusted adult.

- ***Warn children that they should not perform any mysterious computing commands they do not understand at the encouragement of others online.***

On IRC in particular a few people have discovered how to take over another person's computer with certain "/" commands and enjoy taking advantage of this. If children have a question about how to do something, they need to be able to ask a teacher or parent.

- ***The most basic rule for both adults and children when on the Internet: if you do not like what you are reading online, stop reading it.***

This rule extends to interaction on MUDs and IRC. Should children find themselves subjected to text that disturbs them, they need to feel empowered to simply remove themselves from the discussion. On MUDs if something is particularly disturbing, people can teleport from the space where they were experiencing difficulty or simply exit the game, then inform a wizard, arch wizard or god (the people who oversee the game) of the difficulty. These people can talk with the offender(s) and ask that they modify their behaviour or kick them off all together. Within IRC the command "/IGNORE(space) (nickname or user@host)" will block all messages from a particular person. In UseNet newsgroups it is easy enough to not bother viewing messages of a particular subject thread or by a particular person.

- ***Teach children to be respectful and tolerant of others online.***

It is very easy when we grow up in a single community to believe that the beliefs we pick up there are everyone's beliefs everywhere. This is not so, and becomes amply demonstrated when you experience the Internet, a place of worldwide diversity. The Internet will not stop being diverse, therefore to enjoy it you will need to learn how to listen and respond to people as respected equals. This does not mean you have to agree with them, but for successful long term interaction, to learn new things and expand one's horizons, such an approach will be important. Think twice before saying anything, honouring both yourself and others.

Daniel Ingvarson is the Director of *schoolsNET*, an Internet Service Provider designed specifically for Victorian schools. Daniel can be contacted via email at <dan@victoria.schnet.edu.au>.

CENSORSHIP AND THE NEED TO DEVELOP POLICY

Phil Davison
Iroquois Ridge High School, Oakville, Ontario, Canada

Student responsibility is one of the corner stones of education. Providing opportunities for students to demonstrate the attitudes and skills that we are trying to inculcate in them requires us to take the risk of students disappointing us. At Iroquois Ridge High School in Oakville, Ontario this philosophy translates into our granting students full access to the Internet.

At our school we began this journey with a group of students and teachers discussing what the key issues were in regard to the use of computers and the Internet in computer labs. Rather than develop a list of all of the evils that students should never be exposed to, or expose themselves to, we opted to focus on the positive. We require that the students use the network 'responsibly' (our full policy on the use of computers in the school is available on our web site located at <http://www.irhs.haltonbe.on.ca>).

A grade 9 student surfing to the Playboy web site knows that such an action is as inappropriate as opening a copy of the magazine in class. On the other hand, a senior student researching an essay on censorship might have a legitimate need to search for information about racists on the Web, and might spend some time looking at the content of a white supremacist's page. The context of the use of the information is critical to how appropriate the information is for use in a school setting. The understanding and application of this concept is at the root of our policy. In requiring our students to be responsible in their use we are requiring them to examine their motivations and the consequences of their actions.

If, as a group, students were not acting responsibly, then Internet access would be cut off. But as long as the majority of students value the access, and respect the need for the expectation of responsibility then we will have a system that works.

On an individual basis there are students who make poor decisions and it is critical that these individuals be made accountable for their actions. To achieve this, the same group of students and staff who developed the policy of responsibility also developed a process for dealing with individuals who do not meet our expectations. A serious issue involving the misuse of the technology is brought before a panel of students and teachers who discuss the infraction, listen to the students and teachers involved, and make a decision as to the appropriate course of action. In the past, students have been reprimanded, had their use of computers suspended or revoked, been removed from computer based courses, and in one case suspended.

We believe at this school that the empowerment of students is a critical step in helping them to develop into responsible citizens. We present them with high expectations and work with them to meet those expectations. The development of our Internet access policy was really a process of outlining a further responsibility we expect our students to live up to. Ensuring that there are consequences for not meeting these expectations that are seen to be fairly applied further reinforces that these responsibilities are important. To date our students have been responsible users of the Internet and continue to enjoy the benefits of the connections it provides.

Phil Davison is the Information Technology Coordinator and an English Teacher at Iroquois Ridge High School, Oakville, Ontario in Canada. Phil can be contacted via email at <Phil_Davison@msn.com>.

BEST COPY AVAILABLE

ARE YOU FEELING THE INTERNET BACKLASH?
OR
FAMILY FRIENDLY DIGITAL LIBRARIES AND BANNED URLS WEEK

Steve Cisler
Manager, Network Outreach,
Apple Computer, Inc., California, USA

I guess it was inevitable: a hydra-headed backlash against the Internet from many sectors: government, religious activists, nationalists, other librarians, and individual critics. However, it is growing in quantity, as is the positive hype in newspapers, television, and magazines.

The *Wall Street Journal* for January 25, 1996 published a front page article critical of the World Wide Web 'For some, the Web is just a slow crawl to a splattered cat', while the classified section of the same paper has two full pages of their growing 'Internet Directory'. The copy explaining the Web in the directory takes a somewhat more enthusiastic view than the front page article. Of course, they are trolling for advertising revenue, not looking for a new spin on the Internet phenomenon.

One critic, known to readers and librarians who have seen him at ALA or state library conferences is Cliff Stoll, author of the very popular *The Cuckoo's Egg* and more recently, *Silicon Snake Oil* wherein he debunks the Internet and the digital good life touted by other writers like Nicholas Negroponte and George Gilder. Many net users considered Stoll a turncoat for being so critical and sent him email to that effect. I caught up with Cliff at the November 1995 Hackers Conference at Lake Tahoe, and he was just as manic as ever, holding animated discussions on 'how to write a book' and his latest neighborhood hack - He built a radar gun, hooked it to his Mac to track the speeders in front of his house and took the printed graphs of the traffic patterns to the city planning folks in Berkeley. Result: speed bumps for his street. I was more interested in how his life had changed since *Silicon Snake Oil* which has a fairly extensive number of references to the uselessness of computers in libraries and schools, among other places. I asked him if he really had backed away from using computers and networks. No, he had merely cut down from six to eight hours a day to about an hour. It was clear he had been a very heavy user, and the book was his way of wrestling and perhaps conquering an addiction to UseNet, email, and the Internet in general.

In person, he is a lot more ambivalent about the views expressed before audiences or reporters, but his condemnation carried a lot of weight because he is so knowledgeable about computers (otherwise he would not be invited to the Hackers Conference).

The more dangerous opposition comes from journalists, many of them behind the learning curve, or those who catch a trend rather late and begin reporting on it belatedly. Few remember Joe Abernathy's article in the *Houston Chronicle* that sensationalized 'porno on the Internet' in 1990, **<http://www.eff.org/pub/CAF/library/library.porn.real>** and they want to write the story as if it is the latest big news. Frequently, they may call the library if they have a public access computer. In one case, they wanted the librarian to find the smut for them so they could write about it! Now that is a real challenge to the mission of the reference librarian: help the person who is specifically hoping to bring adverse attention to your library because of material somewhere on the Internet. The advice I have been giving people I address (or at least those who understand the Internet) is to take a journalist (or elected official) to lunch and let them know why you feel the Internet is a positive force. This is one way of counteracting some of the unbalanced reporting that is still showing up in articles about the Net. I believe that ALA should have a collection of short success stories to share with other libraries, with publicists and politicians. For a good example, the FARRNET collection of 51 stories from 50 states and the District of Columbia. You can still use gopher to take a look at the stories: **<gopher:// gopher.cni.org:70/11/cniftp/miscdocs/farnet>**.

Backlash has been increasing from different governments. Some see the Internet as yet another manifestation of Western technology and global cultural trends that weaken or fragment national cultures and contribute to the moral decay of their societies. At the extreme you have countries like Saudi Arabia which has the resources to wire up their country and give every bedouin a mobile device for communications, but they are still not on the Internet. They are quite worried about the

kinds of information available to their citizens. When I lectured in Istanbul, Turkey, at IFLA, the Turks did not like a number of the Mediterranean area web sites that I chose to illustrate how the WWW can be used for religious and political propaganda purposes, but that was the point of my lecture.

In Germany, a prosecutor in Bavaria has compelled CompuServe to drop hundreds of UseNet discussion groups because of sexual content. This has not only affected German subscribers but others as well, until the company figures how to segment access in an appropriate way for a whole country. As we go to press, US web sites with Jewish holocaust revisionist literature and propaganda are being blocked by German Internet service providers. While revisionist material is legal in the United States, it is not in Germany.

Many countries in Asia have been building extensive data networks with the goal of bringing the Internet into homes and schools. When I was in Thailand in January 1995, the royal princess' use of email was covered in the English language papers. At the same time, the Thais, who genuinely love their royal family, were quite worried about outside criticism of Thai royalty, and about the constant linkage of Thailand with sex vacation tours. Singapore is always treated in the press as an Orwellian autocracy where the Net may run on time, but you have to watch what you say, do, or read. The truth is that Singapore is lagging behind the United States in repressive legislation to control the Internet.

At the 1995 Internet Society conference in Honolulu, I met Peng Hwa Ang, a lawyer from Singapore. We had been corresponding since 1994 after I sent him my paper on 'Protection and the Internet', and he had undertaken an Internet study for the National Computer Board in Singapore. As a lawyer and lecturer in mass communications, Ang made a number of interesting points in his lecture and his paper, 'Censorship and the Internet: A Singapore Perspective', at <**http://info.isoc.org:80/HMP/PAPER/132/abst.html**>, citing 'uninhibited' reporting about racial issues and the riots that followed, the government believes that censorship of the media is necessary. Singapore wants to be the telecommunications hub, not just for southeast Asia, but for the whole world, yet it also wants to control, among other things, the Internet even as it tries to spread access within the city-state.

Because of labor shortages they cannot afford to hire the number of human censors that would be required. At present there are different servers for the staff at the National University and the students. It is obvious they would want to extend this model to the general population, who could see some, but not all the information flowing through the Singapore node. In legal terms, Singapore has chosen to treat the Internet as a broadcast service and regulate it accordingly. And this trend is what was significant for us in the United States: view the Internet not as a digital equivalent of the world of publishing, book stores, libraries, and readers with First Amendment rights afforded to printed material, but as a broadcast network with performances, shows, sponsors, and much more government control that is tolerated by the relatively free print environment.

In February 1996, Congress passed the Telecommunications Act of 1996. Title V is known as 'The Communications Decency Act of 1996' and was opposed by many organizations such as ALA, Electronic Privacy Information Center (ALA's Judith Krug is on the advisory board) <**http://www.epic.org**>, and the Center for Democracy and Technology <**http://www.cdt.org/**>, and ad hoc groups that organized on the Net around this issue. It was backed by a number of groups including the Christian Coalition which, in May 1995, released its 'Contract with the American family' and specifically addressed the problem of pornography on the Internet. This was one of the motivating forces behind my talk on 'Children and the Internet' at ALA last summer. I suggested that librarians take time to explore and be familiar with the material that is still relatively accessible and not just say they can't find the objectionable material. It's there, but there has been considerable debate about how much, whether it's harmful, and what should be done as more schools are hooking into the Net.

The bill's author was Senator Exon of Nebraska who admitted he did not know much about computers or the Internet, and many critics of the bill say that much of the problems stem from the legislators' ignorance and the heavy influence of the Christian right. The full text of the bill and the section is available many places, but I recommend the EPIC site because it has related material of

BEST COPY AVAILABLE

interest to librarians. The relevant sections are about 32 kb long. It begins with a description of a cybersmut criminal:

> ...whoever initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person...

Now, just days after the passage of the bill, reaction has been swift. Opponents are pushing for test cases in courts, acts of online mourning (making the site's web pages with a black background and white text), and wide use of what in radio broadcasting would be deemed obscene language.

In the other camp we have a group called Oklahomans for Children and Families (OCAF) posting a 100kb guide for the public and law enforcement personnel on how to stop pornography on the Internet. For a copy send an email message to **<noporn@mailback.com>** with no subject and no body. The ascii file will be mailed to you. By the time you read this I'm sure it will be on a number of web sites as well. Try searching under OCAF in **<http://altavista.digital.com/>**. OCAF's focus is on the local Internet Service Provider which in a few cases may even be the local library, but because of the access points available in many university and public libraries, readers should be aware that OCAF sympathizers may use the information in this document to challenge the service you are providing to citizens and students. The OCAF document contains basic information on what they consider illegal, how some basic Internet tools work, and the methods they recommend to resolve what they see as a problem. I suppose that if you pass muster, you might be designated a Family Friendly Digital Library. If you don't, you can start your own exhibit for Banned URLs Week.

Undoubtedly, ALA lawyers, as well as others representing your library, will be scrutinizing the bill and planning what course to follow. Some online activists are planning test cases in the hopes of having the anti-porno sections invalidated in court. Currently, there is a lively discussion of what course Internet Service Providers should take in the light of OCAF's aggressive action.

The World Wide Web community has been working on a technical solution to the problem of controversial material on the Internet. Much of the activity started when the Internet community realized the threat from the Exon amendment many months ago. Whether this has much relevance in the aftermath of the restrictive legislation that will become law remains to be seen. The WWW Consortium (W3C) includes a working group called PICS (Platform for Internet Content Selection), whose goal is 'to develop an easy-to-use Internet content labeling and selection platform that empowers people worldwide to selectively control online content they receive through personal computers' at **<http://www.w3.org/pub/WWW/PICS/>**. It is being billed as a viewpoint-neutral, voluntary solution for the labeling of content on the Internet. Because the Internet has so many different kinds and grades of information and data, many people are looking for rating systems as well as easy-to-use search tools as a means of getting what they need from file servers and web sites around the world. It is time for librarians to take a new look at the role of rating schemes in the networked world where libraries are knowledgeable but relatively uninfluential players. To embrace rating systems as a complete solution is no more realistic than to condemn them as just another form of censorship, but it is important for our profession to be included in the ongoing and rapidly changing discussion.

Originally published under the title 'Are you feeling the Internet backlash?' in Library Journal 121 (7): 25-26. April 15, 1996.

Steve Cisler is Manager of the Network Outreach, part of the Advanced Technology Group of Apple Computer, Inc. in Silicon Valley, California in the United States. Steve can be contacted via email at <sac@apple.com>.

DEVELOPING A SCHOOL INTERNET MANAGEMENT PLAN

Jack Gilding
Project Manager, CIRCIT

Welcome to my virtual presentation. I'd actually rather be in some other virtual room discussing something interesting like "Home-School Links" or "Cooperative Planning & Teaching". But since we're "here" we should address the topic in hand.

The topic I was given for this paper was "Developing a School Management Plan for dealing with controversial material on the Internet". I have been put in the "Censorship and the Internet in Schools" stream because last year CIRCIT prepared a paper for the (soon to be non-existent) Schools Council on *Management of Student Access to Controversial Material on the Internet*. You can read the Executive Summary online and order the full report from the Australian Government Publishing Service (AGPS) - details are available from the project home page at <http://teloz.latrobe.edu.au/circit/schome.html>.

The issue of controversial material is a real one (if only because the media has made it so) and schools do need to think about and plan how they will deal with it. But don't whatever you do, treat it as the main issue you have to deal with, and in fact don't deal with it as a separate issue, it is one aspect of management of student access.

LEGAL ENVIRONMENT

Regulation of Internet content is a hot political issue. In Australia, the major current initiatives are enquiry by the Australian Broadcasting Authority and proposed NSW legislation. If you want to find out more about these issues, a good starting point is Roger Clark's 'Regulating the Net' page at <http://www.anu.edu.au/people/Roger.Clarke/II/Regn>.

Existing legislation and proposed new government action will set a general context and minimum standards of regulation which will apply to everyone, but obviously many schools will feel the need to take additional action to manage student access to the Internet and particular types of content.

WAYS OF MANAGING ACCESS

The Schools Council research identified two main categories of ways in which schools managed student access to the Internet: organisational and technological.

Organisational means include:

- supervision
- signing a register before using a computer with Internet access
- Acceptable Use Policies
- student contracts
- working with parents to develop shared responsibility
- placing reliance on student responsibility.

Technological mechanisms include:

- vetting material (eg incoming and outgoing email)
- using a specialist service provider who limits access to certain sites or newsgroups
- restricting access to particular Internet tools (eg IRC, newsgroups)
- blocking access to specific sites (either at school or at the service provider level)
- downloading specific Internet information for student access (as opposed to allowing students direct access to the Internet)
- keeping log files and running random checks of sites students have accessed

BEST COPY AVAILABLE

- using filter software (these programs have not been widely used in schools and are generally not regarded as sufficiently reliable for use as the main mechanism to control access to inappropriate material.

Different schools use different combinations of these mechanisms, and schools interviewed were generally happy with the arrangements they had in place (which in some cases involved only organisational arrangements).

So you can see that there is quite a range of mechanisms available, but you will have to make your own decisions about which of these suit the requirements of your school.

WHERE TO START?

You can't really learn about the Internet by reading about it, you have to do it. So an important part of developing a Management Plan is for a range of people in the school to have had some time experimenting with and exploring the Internet. There are a number of ways you can do this:

- Put a computer with a dialup Internet account in the library and/or staff room. Run hands on familiarisation sessions for staff and let them explore.

- Give staff with home computers access to a dial up account, and perhaps have a modem loan scheme so they can explore at leisure.

- Purchase a portable computer and modem which can be loaned out to staff.

- Visit other schools that are using the Internet extensively (but be sensitive to the many demands that are placed on people in these schools).

- Make sure students are involved. Some students may well be a source of technical expertise you can draw on. Many students will have ideas about the way the Internet can be used positively in areas of interest to them.

- Visit sites on the Internet which give examples of the ways the Internet can be used in schools. Australian sites include:

  - the Victorian DoSE's ***SoFWeb***
    <http://www.dse.vic.gov.au>

  - the ***ACT Education Information Network (ACTEIN)***
    <http://freenet.actein.edu.au/acteinnew/actein.html>

  - *OzKidz* from Ipswich in Queensland
    <http://www.gil.com.au/ozkidz/>

  - ***oz-TeacherNet***
    <http://owl.qut.edu.au/oz-teachernet/>

  - For overseas sources try ***Web 66*** at **<http://web66.coled.umn.edu/>** and the Schools or Education section of various Internet Directories - for example the ***Yahoo K-12 Page*** at **<http://www.yahoo.com/Education/K_12/>**.

- Run parent Internet familiarisation nights. Your local computer supplier may be able to arrange this - both Microsoft and Apple have presentations available. But make sure it's not just a sales pitch and that parents get a chance to try for themselves.

BEST COPY AVAILABLE

WHAT SHOULD BE IN A PLAN?

Make sure all subject areas in the school are involved. The Internet is a general tool, it should not be seen as related fundamentally to the technology and computer studies areas.

Issues you will need to consider in developing a Management Plan include:

- **Do you wish to use an Internet Service Provider who will provide some level of management of what content can be accessed?**
- **Do you want to restrict access to certain Internet tools (eg Internet Relay Chat)?**
- **Where should Internet access be available? In all classrooms, in the library, in a multimedia resource centre? (But *not* in the computer room if the room is seen as primarily for teaching about computers.)**
- **Who has access to email? Are there separate accounts for individual teachers? For grade levels? For individual students?**
- **What organisational arrangement will govern the sending and receipt of email by students?**
- **Is the school planning to publish material on the World Wide Web? If so how will this material be authorised?**
- **Should students be allowed unsupervised access to the Internet? At what age? As an essential part of their activities or as a privilege which can be withdrawn?**
- **Can parent veto their children having access to the Internet?**

CONCLUSION

Management of student access to the Internet is not fundamentally a technical issue (although you should familiarise yourself with the basic issues around the technology).

The Internet is a tool which you can use. It is a powerful tool, and one which will, over time, change the way you view teaching and learning. But it is still a tool and you should decide how you want to use its potential in the context of your school's educational philosophy and approach.

Disclaimer
The views expressed in this paper are the personal views of the author. They are not an official statement of a CIRCIT position. They are informed by (among many things) the research CIRCIT did for the Schools Council, but they are not intended to be a summary of that research, and are certainly not views endorsed by the Schools Council.

At the time of writing this paper, **Jack Gilding** was the Project Officer for CIRCIT in Victoria, Australia. The CIRCIT Home Page can be located at<**http://teloz.latrobe.edu.au/circit/**> and the Schools Council Project can be located at <**http://teloz.latrobe.edu.au/circit/schome.html**>.

BEST COPY AVAILABLE

MANAGEMENT OF STUDENT ACCESS TO THE INTERNET: ISSUES AND RESPONSIBILITIES *

Ken Dillon
School of Information Studies, Charles Sturt University,
Wagga Wagga, NSW, Australia

INTRODUCTION

This paper will examine some of the major management issues relating to the provision of Internet access to students in schools. In particular, the role of the teacher librarian in relation to student access to the Internet (including such issues as censorship, the use of 'filtering' software and the adoption of 'Acceptable Use Policies') will be addressed.

The role of the teacher librarian in a networked information environment differs radically from the traditional role to which school library users have become so accustomed. The fundamental role of the teacher librarian in a networked school should not change from meeting the information needs of users and facilitating information literacy development. What will change is how information services are provided, the nature of the collaborations between teachers and teacher librarians and how information as a strategic resource in schools is managed. Like information technology literate classroom teachers, teacher librarians will increasingly become the 'guide on the side' rather than the 'sage on the stage'. At the same time, the function of the school library will also shift - from 'just in case' storehouses of information to 'just in time' suppliers of information.

As part of the re-thinking associated with the changing role of the teacher librarian, some commentators have foreshadowed a change of nomenclature from 'teacher librarian' with responsibility for the 'school library program' to, for example, 'information services facilitator' or 'director of information services' with whole school responsibility for an 'information services centre' or 'information services unit', or similar (Barron, 1995; Hay and Kallenberger, 1996). The reasons for this shift in emphasis vary between its proponents but ostensibly the basis of such a move lies in the need for 21st century schools (like other information-based organisations) to be more efficient managers of information.

For example, Hay and Kallenberger (1996) caution that the creation of the position 'director of information services' will result not merely from combining the roles of teacher librarian and computer coordinator into one position of responsibility. In an 'informed school' such a view is too narrow and does not take into account the need for management of information on a whole-school basis. A teacher librarian or information technology studies coordinator might be part of the 'information services unit' along with others employed on either a full-time or part-time basis, eg. programmer, editor, computer technician, library technician, and so on - the mix would depend on the circumstances of the individual school. In fact, their model suggests that a complete re-think of existing school structures and management practices is long overdue.

STUDENT USE OF THE INTERNET

One of the main problems that members of many school communities envisage with Internet access is that of student access to 'unsavoury' information, particularly pornographic and violent material. A second, perhaps even more disturbing problem relates to personal security of student users on the Internet. The potential for paedophiles, for example, to 'meet' potential victims online in order to arrange real-time meetings is of particular concern. While such concerns are obviously valid, they need to be kept in perspective. Incidents of this nature sell newspapers and boost television news/current affairs ratings. We can be certain that the media relish these kinds of stories and if

* Note: This paper is a revised and updated version of the original paper presented at VC'96.

coverage of them is not level-headed and responsible, the resultant media hype can be very damaging to proponents of Internet access for schools.

In short, it should be understood that it is an unfortunate fact of life that many of these incidents occur on a much more regular basis in 'real-life'. In most communities exposure to pornographic and violent images, for example, is only as far away as the nearest newstand and video outlet. The degree of 'interactivity' accorded by the Internet is nothing like that available from television, video or even telephone. In this regard, the soon to be released joint report from the Australian Broadcasting Authority and the Office of Film and Literature Classification (1996) should be of interest. The report will make recommendations about the desirability of an Australian 'code of practice' for online services. Also known as the 'Online Services Investigation', the report will be made available on the ABA Home Page <**http://www.dca.gov.au/aba/hpcov.htm**>.

There is a common misconception about the amount of 'controversial material' on the Internet. Spalding, Gilding and Patrick (1996) found that few schools reported incidents of students stumbling across pornography and the like. Ingvarson (1996) and his colleagues at schoolsNet, a Melbourne-based Internet Service Provider (ISP) specialising in education, set out to find out how much potentially 'controversial material' was really out there:

> Hands up all those who have looked for pornography on the Internet (many people have because of all the media attention on it). I thought I would find out. We have 27 years of Internet experience in our building and some of the best netsurfers around. So armed with keywords like nude, erotic, sex, bombs, and many more we set out on a 36 hour hunt for the dark side of the Internet. We searched over 11 million pages of the World Wide Web, gopher and FTP. We found 3136 sites which matched our keywords. These were made up of a vast array or sites, including: magazines, self-help pages, community information, and academic discussions. There were 45 indexes to other pornographic sites. These indexes proved to be very frustrating. On some of the lists more than 60% of the sites listed were either no longer available, required you to pay for the images, or just never responded. Of the others many were slow, and the pictures of poor quality and mainly of the nude titillation variety.
>
> There was almost a sigh of relief when the first pictures of people having intercourse were uncovered -- one site with more than 12 hard core pictures. It was a number of hours till we found any more.
>
> Out of the entire search only eight sites were found which had pictures which would be considered as hard core pornography -- four of these sites had less than five pictures.
>
> There were a considerable number of sex shops and phone sex sites (which advertise traditional phone sex) -- these would describe products and occasionally have crude selling lines. Most, however, had few erotic images at the site. Some would provide you with titillation of one image and you would have to put in your credit card number to get any more pictures.
>
> In total the number of sites which had considerable pornographic material freely available and easily accessible was less than 100. Out of 11,000,000, that's a percentage of 0.001.

MANAGEMENT OF STUDENT ACCESS

There are a number of different techniques for managing student access to the Internet. In their study of selected Australian schools, Spalding, Gilding and Patrick (1996: xii-ix) identified the following 'wide variety of mechanisms and arrangements to manage student access to the Internet':

- organisational arrangements
  - supervision;
  - signing a register before using a computer with Internet access;

BEST COPY AVAILABLE

- Acceptable Use Policies (AUPs);
- student contracts;
- working with parents to develop shared responsibility; and
- placing reliance on student responsibility.

- technological mechanisms
  - vetting material (eg. incoming and outgoing email);
  - using a specialist service provider who limits access to certain sites or newsgroups;
  - restricting access to particular Internet tools (eg. Internet Relay Chat, newsgroups);
  - blocking access to specific sites (either at school or service provider level);
  - downloading specific Internet information for student access (as opposed to allowing students direct access to the Internet);
  - keeping log files and running random checks of sites students have accessed; and
  - using filter software (these programs are relatively recent, have not been widely used in schools and are generally not regarded as sufficiently reliable for use as the main mechanism to control access to inappropriate material).

This paper will focus on two techniques which are attracting the attention of schools: 'Filtering' software and Acceptable Use Policies (AUPs).

Filtering software

There are a number of software packages specifically designed to limit student access to potentially controversial material on the Internet. Producers of software such as Surfwatch, CyberPatrol, Net Nanny and the like claim that their software can be customised to 'filter' out objectionable material. The extent to which this is achieved is dependent on a number of factors including the techniques used to 'block' or exclude material, how active users are in recommending 'unsavoury' sites (most producers have a reporting mechanism included as part of their Home Page on the WWW), how up-to-date the list of excluded sites is and how clever the maintainers of blocked sites are in getting around the software. Allison and Baxter (1995) consider this use of intelligent software to filter information a 'technological fix' and question the feasibility of software filters in the absence of a broad-based system of Internet content classification:

> Reliable, intelligent software filters are technologically infeasible. Although one can envisage crude filters for text, based on keywords, general filters for other digital materials are infeasible. For example, the required sophistication for image processing software to identify offensive digitised video images is not likely to be available in the foreseeable future. The same applies to audio. Intelligent software filters are at best a partial solution. The coming multimedia age will make them an increasingly less complete solution.

Commercial software producers have not been deterred, however, and the number of packages on the market is on the increase. Some of the more popular packages include:

SurfWatch from Spyglass Inc.	**<http://www.surfwatch.com>**
Net Nanny from Trove Investment Corp.	**<http://www.netnanny.com>**
Cyber Patrol from Microsystems Software	**<http://www.microsys.com>**
CensorNet from ATS International Pty Ltd	**<http://www.ats.com.au>**
CYBERSitter from Solid Oak Software	**<http://www.rain.org/~solidoak>**
Net Shepherd from Net Shepherd Inc.	**<http://www.shepherd.net>**

The titles chosen for these pieces of software conjur up protective images. This is not a coincidence! Terms like 'nanny', sitter', 'shepherd' and 'patrol' suggest that guidance, advice and even comfort

forthcoming for the helpless child lost along some off-ramp of the electronic superhighway. This may be why these producers have had so much trouble trying to shake off accusations that their products actually constitute a form of online censorship: as Williams and Dillon (1993) point out, the idea of 'protection' is one of the main, if not the main, motivation of would-be censors of school library materials. For a more detailed discussion of the limitations of intelligent software filters in the school and home, consult McKenzie (1996).

Internet Service Providers (ISPs) can also 'limit access' to selected sites on an ongoing basis. In Australia, schoolsNET, for example, uses software called CensorMan to block access to sites in the schools it services. Ingvarson (1995) points out that the decision to block one or more sites is a school decision and not a decision of the ISP. ISPs are merely providing a service to schools. Not only is it impossible for ISPs to guarantee blockage of potentially controversial sites for schools due to the sheer number of new sites appearing every day, it is also difficult to predict the types of sites schools want blocked. For example, some seemingly innocuous sites such as the NBA Home Page have been the subject of requests for blocking by schools because of their 'potential for wasting valuable student time online'.

Acceptable Use Policies (AUPs)

In addition to the use of intelligent software filters, teacher librarians and other staff have attempted various means of 'filtering' student access. The most common of these methods is supervision of access. Clearly this is not a practical solution! Another idea is to establish a menu of, for example, servers from which students can select desired 'pathways'. Specialist educational providers of access to the Internet may provide a list of 'bookmarks' on the World Wide Web which they recommend as educationally useful. This strategy is also used by some schools. Another method is to 'download' a selection of (potentially) useful sites for a designated need, eg. an assignment topic and have students conduct their searches of those sites. Of course, some of these measures are fanciful as students will quickly work out how to navigate their way to other parts of the Internet.

One of the most popular options for management of student access to the Internet is the adoption of an Acceptable use Policy (AUP) which Rumbagh (1994) defines as a:

> ...written agreement, signed by students, their parents, and teachers, outlining the terms and conditions of Internet use. It specifically sets out acceptable uses, rules of online behavior, and access privileges. Also covered are penalties for violations of the policy, including security violations and vandalism of the system. Anyone using a school's Internet connection should be required to sign an AUP, and know that it will be kept on file as a legal, binding document.

For some readers, the foregoing description may be a little over the top. As Spalding, Gilding and Patrick (1996) report, however, many Australian schools are moving toward this course of action. Rumbagh goes on to contend that the 'school solicitor' may need to scrutinise any AUP in the drafting stage. While such a suggestion may reflect the litigious nature of US society (school policies including selection policies for school libraries are signed 'legal' documents in many US school districts), most existing Australian policies are less formal and are clearly designed to apportion *responsibility* for using the Internet in schools. The bottom line is that the responsibility for allowing access should rest with students and/or their parents and not with the ISP, educational authority, school or individual staff members. In fact, Spalding, Gilding and Patrick (1996: 32) warn that even systems based on parental permission are really short-term measures:

> The notion of parental permission, however, will become increasingly difficult as more students use the facility. The students' who do not have parents' permission will become disadvantaged in terms of restricted access to a resource. Some schools believe this is, in fact, an interim phase and in due course it will not be realistic to have a situation where some students, at the discretion of their parents, will be denied access. It will be more a question of parents understanding what is being offered, what particular controls that particular school has in place and feeling reassured about the capacity of their child to

BEST COPY AVAILABLE

handle the consequences of an inadvertent exposure to controversial material. The bottom line, as one school put it, is that parents may choose to send their children to another school.

In the teacher librarianship strand of this conference the consensus of opinion among participants in the 'Censorship and the Internet: Problems and Solutions' topic has supported such a view: responsibility for searching the Internet should lie with students and/or parents. An 'information session' for parents about using the Internet as a research tool was a widely accepted strategy for alleviating actual or potential concerns of parents. Davison (1996) describes an Internet access/management strategy for secondary schools where the onus of responsibility for sites visited lay with the individual student who is accountable for his/her actions. Similar to many other schools, there are penalties for infringers. However, this model addresses one of the main criticisms of Internet access/management in many schools - lack of student involvement, eg. in the formulation of AUPs or in the determination of appropriate penalties for infringements.

Does an 'Acceptable Use Policy' (AUP) differ from a School Policy for student access to the Internet? The following suggestions have been adapted from McKenzie (1995).

- In basic terms, AUPs help to define acceptable behaviors by student and staff users of information systems, while school policies take the matter much further. AUPs were designed to satisfy the regional networks that some schools join when driving onto the Electronic Highway.

- School policies also describe acceptable student behaviors, echoing the content of AUPs, but they tie those standards to the school's policies on student rights and responsibilities, drawing connections, for example, with the school policy and procedures on locker searches and a student's rights to privacy and freedom to read. They tie consequences and procedures to those already in effect.

- In addition, a sound school policy takes a position on access to potentially controversial information and relates these new information sources to pre-existing policies on curriculum and the selection of curriculum materials, outlining clear expectations for staff supervising student use.

- Finally, a comprehensive set of policies would also outline staff responsibilities and rights as employees using these utilities.

Hanson (1994) offers the following 'Acceptable Use (Ethics) Agreements' Checklist' as a guide for formulating policy at the school level:

- confirm student has read it and understands it
- may or may not include parent permission
- use of the Internet is a privilege, not a right
- respect for limited network resources
- proper account management (quotas)
- nothing is really private
- remain on distant systems only as long as you need to
- adhere to time restrictions of archive sites
- check for and adhere to copying and licensing agreements
- lurk on a listserver or newsgroup before posting
- insert your address at the bottom of messages
- be careful with sarcasm and humour
- learn the difference between a listserv's admin and discussion addresses
- rarely reply to the list, opt for replying to the poster
- never share your account with anyone
- use a cryptic password
- be alert for unsuccessful login attempts and last login flags.

policies

a number of collections of sample school policies for student access to the Internet and AUPs for libraries. Some of the most well known include (in no particular order):

1. AskERIC
<http//ericir.syr.edu/Projects/ICONN/CurriculumConnections.html>
Look under Intellectual Freedom and Acceptable Use Policy.

2. *Texas Education Network (TENET)*
<http//www.tenet.edu/tenet-info/accept.html>
Look under TENET Acceptable Use Policy.

3. *Classroom Connect*
<ftp://ftp.classroom.net/wentworth/Classroom-Connect/aup-faq.txt>
Consists of FAQs (Frequently Asked Questions) about AUPs as well as suggested sources. Periodically updated and made available via email.

4. *Acceptable Use Policies (Rice University)*
<http://www.rice.edu/armadillo/acceptable.html> and
<gopher://riceinfo.rice.edu:1170/11/More/Acceptable>
Includes a wide range of sample AUPs and discussions about Internet censorship.

5. *Bellingham Public Schools*
<http://www.bham.wednet.edu/policies.htm>
Look under Board Policies then under sub-division Internet.

6. *The Internet Advocate*
<http://silver.ucs.indiana.edu/~lchampel/netadv.htm>
Look under Introduction then under sub-division Develop an Acceptable Use Policy.

7. *K-12 Acceptable Use Policies*
<http://www.erewon.com/k12aup/>
Includes templates for developing AUPs.

8. *Southern Regional Acceptable Computer Use Policy*
<http://150.216.8.1/schofed/lset/AUP.HTM>
Look under Acceptable Computer Use Policy.

9. *Arkansas Public School Computer Network*
<http://www.k12.ar.us/ecc.htm>
Look under Current Local (Arkansas) Information then sub-division Network Appropriate Use Guidelines (PDF File).

10. *Karen's Kitchen: The Freedom Pages*
<http://www.intac.com/~kgs/freedom/policies>
Look under Sample Library Policies.

11. *California Department of Education Goldmine*
<http://goldmine.cde.ca.gov/WWW/Technology/Ed_Tech/Policy.html>
CDE's Acceptable Use Policy and District Guidelines.

12. *Avoiding Ethical Potholes: Acceptable Use Policies*
<http://www.ucalgary.ca/~mueller/aup.html>
Includes a range of sample AUPs, links to other collections of AUPs and related sites.

BEST COPY AVAILABLE

Of course, URLs can and do change so it is wise to re-check your bookmarks from time to time. The preceding URLs were accurate as of June 28, 1996. Comments about and suggestions for additions to this list and the list of available intelligent software filters are most welcome.

CONCLUSION

The whole question of student access to the Internet is a perplexing issue. Media 'hype' has certainly fuelled the debate over access to the Internet for school-age children and sown the seeds of doubt in the minds of some members of school communities about making access to the Internet a reality/priority. For teachers and teacher librarians, there are a range of crucial issues to do with equity of access and effective harnessing of the Internet for teaching and learning, to consider. As part of the school's information technology team, the teacher librarian/information specialist has a pivotal role to play in making access to, and effective use of, this valuable resource a reality for all members of the 'information literate school community'.

REFERENCES

Allison, L. and Baxter, R. (1995) *Protecting our innocents*. Melbourne: Department of Computer Science, Monash University. (Technical Report 95/224)

Barron, D.D. (1995) Information services facilitators to replace school library media specialists. *School Library Media Activities Monthly*. 11, 8, 48-50.

Davison, P. (1996) Censorship and the need to develop policy. Paper presented at *Schooling and the Information Superhighway Virtual Conference*. June 3-9.

Hanson, W. (1994, November 15) RE: Student access to the Internet. School Library Media & Network Communications [Online]. Available email: **<listserv@listserv.syr.edu>**

Hay, L. and Kallenberger, N. (1996) The future role of the school information services unit in the teaching/learning process. Paper presented at *Electronic Networking and Australasia's Schools*, Sydney, April 11-13. Available WWW: **<http://www.itec.com.edu>**

Ingvarson, D. (1995) Censoring the Internet: the practicalities. Paper presented at *The Information Highway and the Nation's Schools* Conference, Sydney, June 10.

Ingvarson, D. (1996) Planning a safe ride on the Superhighway. Paper presented at *Schooling and the Information Superhighway Virtual Conference*. June 3-9.

McKenzie, J. (1995, 9 May) FNO May 95: Board policies for Internet. School Library Media & Network Communications [Online]. Available email: **<listserv@listserv.syr.edu>**

McKenzie, J. (1996, March-April) From Now On: A Monthly Electronic Commentary on Educational Technology Issues. Available WWW: **<http://www.pacificrim.net/~mckenzie>**

Rumbagh, S. (1994) Acceptable use policies: defining what's allowed online, and what's not. Classroom Connect, Wentworth Worldwide Media. Available WWW: **<http://www.classroom.net>**

Spalding, B., Gilding, J., and Patrick, K. (1996) *Management of student access to controversial material on the Internet*. Canberra: Australian Government Publishing Service.

Williams, C.L. and Dillon. K. (1993) *Brought to book: Censorship and School Libraries in Australia*. Port Melbourne, Vic. : ALIA Press/DW Thorpe.

BEST COPY AVAILABLE

...Sites

...(Platform for Internet Content Selection)
<http://www.w3.org/pub/WWW/PICS>

PICS, the Platform for Internet Content Selection, is designed to enable parents, teachers, or administrators to block access from their computers to certain Internet resources, without censoring what is distributed to other sites. It draws on two unique features of the Internet.

First, publishing is instantaneous, world-wide, and very inexpensive, so it is easy to publish rating and advisory labels. Labels and ratings already help consumers choose many products, from movies to cars to computers. Such labels are provided by the producers or by independent third parties, such as consumer magazines. Similarly, labels for Internet resources could help users to select interesting, high-quality materials and could help supervisors to block access to inappropriate ones.

Second, access to Internet resources is mediated by computers that can process far more labels than any person could. Thus, parents, teachers, and other supervisors need only configure software to selectively block access to resources based on the rating labels; they need not personally read them.

In August 1995, representatives from twenty-three companies and organizations gathered under the auspices of MIT's World Wide Web Consortium to discuss the need for content labeling, especially for use with selection software. Faced with the obvious desire of some parents and other users to control what they or their children have access to, the companies felt that such tools were important to the continued growth of Internet and on-line service use in homes, schools, and businesses. The attendees also hoped to offer a positive alternative to US government regulation of on-line content, which would dampen free speech. The group decided to develop a technical infrastructure that would support label distribution and selection software. PICS, the fruit of the group's work, establishes conventions for label formats and distribution methods, without dictating a labeling vocabulary or who should pay attention to which labels. It is analogous to specifying where on a package a label should appear, and in what font it should be printed, without specifying what it should say'.

Ken Dillon is Lecturer in Teacher Librarianship at the
School of Information Studies, Charles Sturt University - Riverina,
Wagga Wagga, New South Wales in Australia.
Ken can be contacted via email at <kdillon@csu.edu.au>.

BEST COPY AVAILABLE